# Customer Technical Bulletin

## CTB-00315 Rev. 002

**Date:** *07/25/17*

**Author:** Service Engineering

**Product:** Referenced in Document **Subsystem:** Microsoft Windows OS

**Subject:** Microsoft MS17-010 – Critical Security Update for Microsoft Windows (4013389)

## Purpose

In March 2017, Microsoft released a security update to address a vulnerability in their operating system. This vulnerability was compromised on Friday, May 12th in a coordinated attack, known as Wannacrypt (aka "WannaCry"), EternalBlue and others. These attacks are utilizing a Microsoft SMB vulnerability, described in Microsoft bulletin MS17-010, to propagate and infect other devices on a network. Hologic is strongly recommending that the Microsoft KB4012212 security patch be applied to Hologic products that use Microsoft Operating Systems to fix this vulnerability.

Vigilance is key in these times to ensure internal systems are never compromised. Having a hardened, resilient network environment that is agile to deal with security compromises is essential. Hologic is committed to monitor these compromises and quickly work to resolve them. At the same time, Hologic recommends incorporating standard security practices that incorporate proactive security mechanisms that deal with emerging zero-day vulnerabilities and exploits,

Hologic has validated the Microsoft MS17-010/ KB4012212 security patch on Hologic products listed below. It is Hologic's recommendation that this patch be applied to both your Hologic and Non-Hologic products.

## Supported Products

The instructions provided in this document apply to the following products:

- Affirm Prone Biopsy System
- AWM
- Dimensions
- Trident
- Windows Selenia
- Cenova
- SecurView
- MultiView

## Customer Suggestions

- Install security update for SMB vulnerability, described in MS17-010, to mitigate propagation to our devices. Instructions for installing the security patch are included in this document.
- Check out Hologic support web portal (http://www.hologic.com/support) for validated Antivirus software for each of the Hologic products. It's recommended that one of these packages be installed on our devices and updated with latest virus definitions.
- Avoid personal activities such as surfing the internet, downloading files, and checking email on Hologic medical devices.
- Block SMB traffic at your network perimeter whenever possible to limit exposure of unpatched devices to the internet and implement secure networking techniques, such as network segregation where appropriate.

## Obtaining the Microsoft Patch

**Microsoft Bulletin for SMB Vulnerability (MS17-010):**

https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

**Specific security patch for Windows 7 32-bit (Trident and Windows Selenia):**

http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.1-kb4012212-x86_6bb04d3971bb58ae4bac44219e7169812914df3f.msu

**Specific security patch for Windows 7 64-bit & Windows Server 2008 R2 (Dimensions, Affirm Prone Biopsy System, AWM, Cenova, MultiView, and SecurView):**

http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.1-kb4012212-x64_2decefaa02e2058dcd965702509a992d8c4e92b3.msu

## Installing the Patch

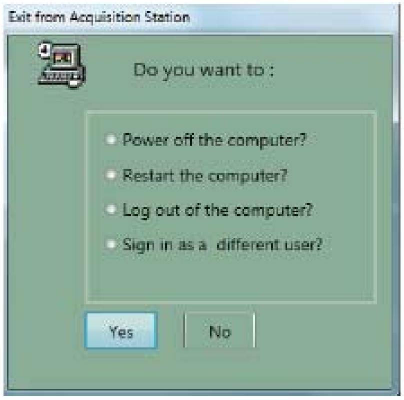
Installation of the patch requires administrator access to the system. Please reference your training material or contact Hologic Support to obtain login credentials.

1. For Hologic systems without automatic login, such as **AWM, Cenova, and MultiView**, log into Windows as an Administrator and skip to step 5.
   ***Note: The default user for AWM is Administrator.***
2. For the **Affirm Prone Biopsy System, Dimensions, and Trident** products, perform the following steps to exit the application and access the Windows desktop:
   ***Note: For any questions or clarification with these steps, please reference the appropriate product User Manual.***
   a. Log out of the application.
   b. Hold the **CTRL** key on the keyboard while clicking **Shutdown** in the application. This should exit the application, instead of shutting down the computer, and allow access to the Windows desktop.

3. For the **Windows Selenia** product, perform the following steps to exit the application and access the Windows desktop:
   ***Note: For any questions or clarification with these steps, please reference the appropriate product User Manual.***

   a. In the application, select **File -> Exit**.

   b. Select **Log out of the computer?** option.



Exit from Acquisition Station

Do you want to :

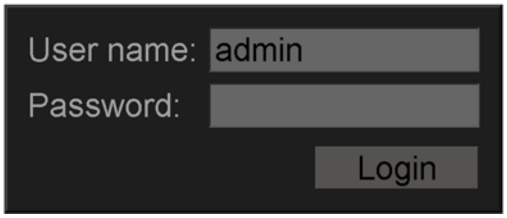
○ Power off the computer?
○ Restart the computer?
○ Log out of the computer?
○ Sign in as a  different user?

   c. Click Yes.

   *d.* At the login screen, log in as the admin user.
   ***Note: The admin user is the account you will use to install the security patch and perform all steps in this document.***

*4.* For the **SecurView** product, perform the following steps to exit the application and access the Windows desktop:

   a. In the application, Login as the admin user



User name: admin
Password:

   b. Select **Exit to Windows** from the menu bar along the right edge of the monitor

   c. Press the Windows key and select Log off to log out of Windows.

   *d.* At the login screen, log in as the administrator user.
   ***Note: The admin user is the account you will use to install the security patch and perform all steps in this document. Please reference your training material or contact Hologic Support to obtain login credentials.***

5. Enable and start the Windows Update service:

Note: Please reference the links in the “Obtaining the Microsoft Patch” for your particular Windows Operating System.

   a. Press the Windows key on the keyboard to access the Start Menu.

   b. In the start menu search box, type **services.msc**.

   c. Click on services.msc displayed in the list above.

d. Find the **Windows Update** service in the list, right click on the service and select **Properties** from the menu that appears. If the service in enable and set to Automatic skip to

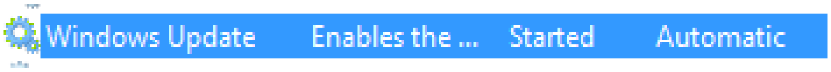
e. Set the Windows Update service startup type to **Automatic**.

f. Click **Apply**.

g. Click **Start**.

h. Click **OK** to close the Windows Update service properties window.

i. In the Services window, confirm that the Windows Update service now has a startup type of Automatic and that its status is Started.



Windows Update Enables the ... Started Automatic

j. Close the Services window.

6. Obtain the KB4012212 security patch (see "Obtaining the Microsoft Patch" section above).
7. Once KB4012212 installation file has been deployed to the product system, start the installation by double clicking on it.
8. Step through the installation dialogs that appear until the patch installation is completed.
9. At the Installation complete window, click **Restart Now**.
10. The computer will restart.
11. If the Windows Update service was enabled in steps above, set it back to a disabled state:

a. Access the Windows desktop using instructions provided in earlier steps.

b. Press the Windows key on the keyboard to access the Start Menu.

c. In the start menu search box, type **services.msc**.

d. Click on services.msc displayed in the list above.

e. Find the **Windows Update** service in the list, right click on the service and select **Properties** from the menu that appears.

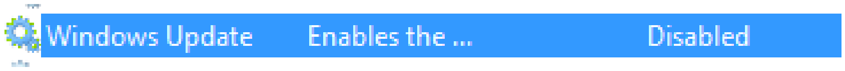
f. Set the Windows Update service startup type to **Disabled**.

g. Click **Apply**.

h. Click **Stop**.

i. Click **OK** to close the Windows Update service properties window.

j. In the Services window, confirm that the Windows Update service now has a startup type of Disabled.



Windows Update Enables the ... Disabled

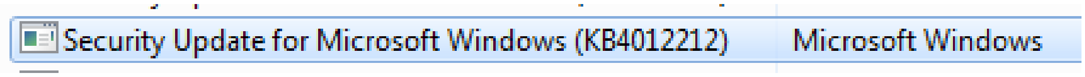
k. Close the Services window.

## Patch Installation Confirmation

1. Login to Windows as administrator. Please see "***Installing the Patch"*** above for login instructions for Hologic products.
2. Press the Windows key on the keyboard to access the Start Menu.
3. In the start menu search box, type **Programs and Features**.
4. Click on Programs and Features displayed in the list above.
5. In the Programs and Features window, click the **View installed updates** link.
6. Installed updates list is presented. Give it a couple minutes to load completely.
7. Confirm that KB4012212 is listed as installed.

***Note: You can sort the list by "Installed On" column to make it easier to see the patches that***

***were just installed.***



Security Update for Microsoft Windows (KB4012212) Microsoft Windows

## Additional Resources

https://www.us-cert.gov/ncas/alerts/TA17-132A

https://www.symantec.com/connect/blogs/what-you-need-know-about-wannacry-ransomware

https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

http://www.hologic.com/support